# UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

A certain cellular phone seized during the arrest of Prince Oduro on February 15, 2022

Case No. 2:22-mj-223

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 USC 1956 and 1957 | Money Laundering |
| 18 USC 1028A | Aggravated Identity Theft |
| 18 USC 1343 and 1344 | Wire Fraud and Bank Fraud |

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Shawn A. Mincks

*Applicant's signature*

Shawn Mincks, Special Agent, IRS-CI

*Printed name and title*

ATTESTED TO ON FACETIME

Sworn to before me and ~~signed in my presence~~.

Date: _____

Norah McCann King

*Judge's signature*

City and state: Columbus, OH

Norah McCann King, U.S. Magistrate Judge

*Printed name and title*

**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF OHIO**
**EASTERN DIVISION**

**AFFIDAVIT**
IN SUPPORT OF A SEARCH WARRANT

I, Shawn Mincks, Special Agent, U.S. Department of the Treasury, Internal Revenue Service, Criminal Investigation, being duly sworn, depose and say that:

## Introduction and Purpose

1. I am a Special Agent with IRS-Criminal Investigation and have been so employed since 2008. I have received specialized law enforcement training at the Federal Law Enforcement Training Center, Glynco, Georgia and additional specialized training from the IRS. My duties as a Special Agent include conducting investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code. I have participated in multiple such investigations, including several investigations related to individuals who launder funds derived from fraud schemes.

2. I am assigned to pursue a federal criminal investigation of Prince Oduro and others. I contend there is probable cause to believe that Oduro committed Bank Fraud, in violation of 18 U.S.C. § 1344; Wire Fraud, in violation of 18 U.S.C. § 1343; Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A; Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); and Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957. I further contend that evidence of such violations, described in Attachment B, is located on or in the item described in paragraph #3 and Attachment A.

3. I make this affidavit in support of an application for a search warrant for a cellular phone seized by IRS-Criminal Investigation during the arrest of Oduro on February 15, 2022. The item is further described as the following and is also described in Attachment A.

   Attachment A

   a. Silver and white iPhone seized during the execution of an arrest warrant on Prince Oduro on February 15, 2022.

4. The device is currently in the possession of IRS-CI located at 401 North Front Street, Suite 375, Columbus, Ohio.

5. The information in this affidavit is either personally known to me based upon my experience, investigative activities, analysis of records and interviews; or it has been relayed to me by other agents and/or law enforcement personnel. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included

each and every fact know to me concerning the investigation. I have set forth only the facts I believe are necessary to support the requested search warrant.

**Evidence of Probable Cause**

**Overview**

6. Through interviews, executions of previous search warrants and analysis of financial and other documentation, I believe the investigation to date tends to show that:

    a. Oduro used his position as an employee of JP Morgan Chase Bank to defraud a JP Morgan Chase Bank customer, in violation of 18 U.S.C. § 1344;

    b. Oduro created PayPal accounts using compromised Social Security Numbers, then Oduro and/or parties known to Oduro defrauded other individuals by transferring funds from compromised bank accounts into the PayPal accounts, in violation of 18 U.S.C. § 1028A;

    c. Oduro laundered the funds received into the PayPal accounts, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and;

    d. Oduro conspired with others to receive and disburse funds derived from other fraud schemes, which were facilitated through interstate and/or international wire communications, in violation of 18 U.S.C. §§ 1956(h); 1956(a)(1)(B)(i); and/or 1957.

7. On February 9, 2022, the affiant filed a Criminal Complaint accusing Oduro of violations of 18 U.S.C. §§ 1344; 1028A; and 1956(a)(1)(B)(i). As a result of the filing of the Criminal Complaint, an arrest warrant was issued for Oduro.

8. On February 15, 2022, the affiant and other agents executed the arrest warrant and apprehended Oduro immediately outside the front door to his residence located at 1663 Crescent Ridge Boulevard, Columbus, Ohio. Upon search incident to arrest of Oduro's person, Special Agent Mike McClelland with the United States Postal Inspection Service found a silver and white iPhone in Oduro's right pocket. The affiant then took possession of the phone. This affidavit requests issuance of a search warrant for the silver and white iPhone.

**Bank Fraud**

9. In 2015, Oduro worked at JP Morgan Chase Bank. According to JP Morgan Chase Bank records, on April 7, 2015, at approximately 5:30 PM, through his employment at JP Morgan Chase Bank located in Columbus, Ohio, Oduro accessed the JP Morgan Chase Bank customer profile of Person 21. Person 21 controlled three bank accounts at JP Morgan Chase Bank: JPMC xx8806, JPMC xx7365, and JPMC xx5884.

10. According to JP Morgan Chase Bank records, at approximately 10:22 PM that same day, a call was made to access JPMC xx8806 from phone number 614-779-8584. This same phone number would be used to access Person 21's accounts on 20 different days between April 7, 2015 and September 25, 2015. Capital One records show that Oduro listed this number as his when he opened a Capital One credit card in October of 2015.

11. PayPal records show that on May 16, 2015, PayPal account # xx1356 (PayPal xx1356) was established in the name of Person 21 using Person 21's Social Security Number. The address 2677 Club Lane Drive, Columbus, Ohio would be added to the account later. Capital One credit card records show that this address was Oduro's address from at least November of 2014 through July of 2015.

12. PayPal records show that between June 29, 2015 and August 27, 2015, PayPal xx1356 was accessed numerous times from IP address 104.230.141.26. This same IP address was used to access a PayPal account in Oduro's name on June 11, 2015.

13. PayPal and JP Morgan Chase Bank records show that between June 29, 2015 and July 24, 2015, $7,000 was transferred from JPMC xx7365 to PayPal xx1356. Person 21 would later dispute these transfers, and the funds would be returned to JPMC xx7365 at a loss to JP Morgan Chase Bank. After the funds were transferred to PayPal xx1356, they were withdrawn in cash via JP Morgan Chase Bank ATMs located in Columbus, Ohio and through transactions at Giant Eagle grocery store locations in Columbus, Ohio.

14. PayPal and JP Morgan Chase Bank records show that on August 17 and August 18, 2015, a total of $5,500 was transferred from JPMC xx8806 to the PayPal xx1356.

15. JP Morgan Chase Bank records show that on August 19, 2015, $8,000 was transferred from JPMC xx5884 to JPMC xx8806 via telephone transfer. The transfer was requested by a caller using phone number 614-779-8584. PayPal records show that on August 20, 2015, an $8,000 transfer from JPMC xx8806 to PayPal xx1356 was attempted but denied.

16. PayPal records show that on August 19, 2015, a check in the amount of $630.00 was issued from PayPal xx1356. JP Morgan Chase Bank records show that on August 31, 2015, Oduro deposited a check issued by PayPal to Person 21 in the amount of $630.00 into JP Morgan Chase Bank account # xx8363 (JPMC xx8363) via an ATM deposit at a branch located in Columbus, Ohio. JP Morgan Chase Bank records show that Oduro opened JPMC xx8363 on June 26, 2015 at a branch located in Columbus, Ohio. He was the only signer on the account.

17. PayPal records show that on August 20, 2015, a check in the amount of $500.00 was issued from PayPal xx1356. JP Morgan Chase Bank records show that on September 24, 2015, Oduro deposited a check issued by PayPal to Person 21 in the amount of $500.00 into JP Morgan Chase Bank account # xx5893 (JPMC xx5893). Bank records show that Oduro opened JPMC xx5893 on September 22, 2015 and was the only signer on the account.

**PayPal Fraud Scheme - Aggravated Identity Theft and Money Laundering**

18. In 2016 and 2017, Oduro used means of identification, including names, social security numbers, and addresses of individuals without their knowledge or consent to open additional accounts with PayPal. Oduro then used the accounts in further violations of 18 USC 1343 and/or 18 USC 1344, as outlined below.

*Person 22, Person 39, and Person 40*

19. PayPal records show that on August 23, 2016, PayPal account # xx0882 (PayPal xx0882) was opened in the name of a business containing Person 22's name. The account was opened using Person 22's Social Security Number.

20. PayPal records show that PayPal xx0882 was opened from IP address 74.135.70.235. This same IP address was used to access the account numerous times between August 23, 2016 and October 1, 2016.

21. FedEx records show that this IP address was used to check the shipping status of a shipment bound for 9262 Worthington Road, Apartment 306, Westerville, Ohio, which arrived on June 24, 2016. Capital One Investing records show that this was Oduro's address in 2016. The same IP address was used to access Oduro's account at Capital One Investing between June 1, 2016 and November 3, 2016.

22. On May 3, 2017, the Grove City Police Department executed a search warrant at 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio. Oduro was present during the execution of the search warrant and later stated to federal agents that he lived at the address at the time of the execution of the warrant. During the execution of the warrant, the Grove City Police Department seized Oduro's phone. IRS-CI later executed a search warrant on the phone. The phone was found to contain a text message conversation between Oduro and "Boppa."

    a. Between September 4, 2016 and September 6, 2016, Oduro and "Boppa" engaged in a conversation on WhatsApp during which time Boppa indicated that he was actively engaged in a romance scam involving Person 39. Boppa told Oduro that he needed a PayPal account to which Person 39 could send money. Oduro provided to Boppa information for PayPal xx0882. On September 6, 2016, PayPal xx0882 received $50 from Person 39. On September 7, 2016, Oduro sent Boppa a screenshot confirming that Person 39 had sent $50 to PayPal xx0882.

23. PayPal records show that on September 30, 2016, $1,000 was transferred to PayPal xx0882 from a USAA bank account belonging to Person 40. Within 90 minutes, the money was removed through an ATM withdrawal and purchases at two Meijer locations in Westerville, Ohio.

24. USAA records also show that $1,000 was transferred to Person 22 from Person 40's bank account. The account was subsequently credited for the fraudulent transfer.

25. MoneyGram records show that on September 30, 2016, Oduro sent $600 to an individual named Abiodun Idris Akinniganyin in Cyprus. "Idris" is further discussed later in this affidavit.

*Person 24 and Person 25*

26. PayPal records show that on August 23, 2016, PayPal account # xx4563 (PayPal xx4563) was opened in the name of a business containing Person 24's name. The account was opened using Person 24's Social Security Number.

27. PayPal records show that PayPal xx4563 was opened from IP address 74.135.70.235. This same IP address was used to access the account numerous times between August 23, 2016 and October 7, 2016. This is the same IP address associated with PayPal xx0882.

28. PayPal records show that on September 11, 2016, someone logged into PayPal xx4563 from IP address 74.135.70.235 and changed the address linked to the account to 9262 Worthington Road, Apartment 306, Westerville, Ohio. As previously stated, Capital One Investing records show that this was Oduro's address in 2016.

29. As previously stated, on May 3, 2017, the Grove City Police Department executed a search warrant at 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio. During the execution of the warrant, the Grove City Police Department seized Oduro's phone. IRS-CI later executed a search warrant on the phone.

30. Oduro's phone was found to contain a text message conversation between Oduro and "Kofi saxy_abena Norway" on September 13, 2016. In the conversation, Oduro told Kofi to look for mail in the name of Person 24 that week. The following day, Kofi sent Oduro an image of an envelope addressed to Person 24.

31. PayPal records show that on October 5, 2016, $1,000 was transferred to PayPal xx4563 from a USAA account in the name of Person 25. Within 90 minutes, the funds were exhausted through ATM withdrawals and purchases at Kroger, Meijer and Wal-Mart.

32. USAA records show that on October 5, 2016, $1,000 was transferred to Person 24 from an account held in the name of Person 25 and her husband. The account was subsequently credited for the fraudulent transfer.

33. MoneyGram records show that on October 5, 2016, Oduro sent $500 to Abiodun Idris Akinniganyin in Cyprus.

34. According to an interview with Person 25's husband, whose identity is known to the affiant, somebody accessed his and his wife's USAA bank account without authorization and transferred the $1,000 to PayPal.

35. According to an interview with Person 24, whose identity is known to the affiant, the Social Security Number used to open PayPal xx4563 actually belonged to his deceased wife. Person 24 also stated that he never had a business with the name indicated on the PayPal account; he never lived in Ohio; he does not know Person 25; and he did not make any transactions in Ohio in October of 2016.

*Person 26 and Person 27*

36. PayPal records show that on March 27, 2017, PayPal account # xx6280 (PayPal xx6280) was opened in the name of Person 26 using the Social Security Number of Person 26 and email address gaydys6@outlook.com. The mailing address associated with PayPal xx6280 was 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio. The account was created from IP address 173.88.108.51. This same IP address would be used to access the account numerous times between March 27, 2017 and April 26, 2017.

37. Charter Communications records show that IP address 173.88.108.51 was assigned to a subscriber at 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio between January 12, 2017 and July 15, 2017. The email address for the subscriber account was jrand76110@gmail.com. The phone number for the subscriber account was 614-966-0372. Apple records show that this phone number belonged to Oduro.

38. On April 26, 2017 at approximately 5:15 PM Central Daylight Time, $1,000 was transferred to PayPal xx6280 from a USAA Bank account in the name of Person 27. All the funds were exhausted within 60 minutes through a JP Morgan Chase Bank ATM withdrawal and transactions conducted at four different Wal-Mart locations, all of which occurred in and around Columbus, Ohio.

39. Person 27 was interviewed and stated that he/she does not know Person 26, and he/she did not authorize the transaction to the PayPal account. He/She noticed the transaction only after receiving his/her monthly statement from USAA. Upon noticing the transfer, he/she had his/her spouse call USAA to report the fraudulent transfer. USAA returned the funds to him/her after approximately a month.

40. As previously stated, on May 3, 2017, the Grove City Police Department executed a search warrant at the 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio. During the execution of the warrant, the Grove City Police Department seized a PayPal card issued in the name of Person 26.

41. As previously stated, Oduro's phone was also seized during the execution of the search warrant by the Grove City Police Department. IRS-CI later executed a search warrant on the phone. The phone was found to contain a text message conversation between Oduro and "Idris" that occurred between April 8, 2017 and May 2, 2017. During the conversation, Oduro and Idris appear to discuss the fraudulent activities involving PayPal, Person 26 and Person 27, including the following excerpts:

a. On April 26, 2017 at approximately 5:16 PM Central Daylight Time, Idris sent Oduro a text message stating, "1k dey there now." Oduro responded, "Yeah on my way to cash out."

    i. As stated in paragraph # 38, PayPal records show that on April 26, 2017 at approximately 5:15 PM Central Daylight Time, $1,000 had been transferred to PayPal xx6280 from a USAA Bank account in the name of Person 27.

b. On April 26, 2017 at approximately 5:24 PM Central Daylight Time, Oduro sent Idris a text message stating, "At work."

    i. As referenced in paragraph # 38, PayPal records show that between 5:23 PM Central Daylight Time and 6:15 PM Central Daylight Time, Oduro expended all funds in PayPal xx6280 through a cash withdrawal and transactions conducted at Wal-Mart.

*Person 28, Person 29 and Person 30*

42. PayPal records show that on April 4, 2017, PayPal account # xx7126 (PayPal xx7126) was opened in the name of Person 28 using Person 28's Social Security Number and email address jrand76110@outlook.com.

    a. This is the same email address associated with the IP address 173.88.108.51 per Charter Communication records as described in paragraph #20.

43. PayPal records show that PayPal xx7126 was created from IP address 173.88.108.51. This same IP address would be used to access the account numerous times between April 4, 2017 and June 9, 2017. As previously stated, this IP address is also linked to PayPal xx6280 and to 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio.

44. PayPal records show that on May 26, 2017 and various dates in June of 2017, PayPal xx7126 was accessed from IP address 104.184.20.152. FedEx records show that this IP address was used to track a FedEx Express package bound for Oduro at 9262 Worthington Road, Apartment 306, Westerville, Ohio from July 11, 2017 through July 14, 2017. The package arrived on July 13, 2017 and was signed for by "P. Oduro." This IP address was also used to access a PayPal account in Oduro's name on June 2, 2017.

45. The Grove City Police Department seized a PayPal card in the name of Person 28 during the execution of the search warrant at 777 Worthington Woods Boulevard, Apartment 215, Columbus, Ohio on May 3, 2017. PayPal records show that on May 26, 2017, after the execution of the search warrant, the card linked to this account was reported as lost. A new card was issued as a result.

46. PayPal records show that on June 8, 2017 at 11:19 PM Central Daylight Time and on June 9, 2017 at 12:01 AM Central Daylight Time, a total of $1,999.00 was transferred

from Person 29's USAA Bank account to PayPal xx7126. Within 35 minutes, $400 was withdrawn at a PNC Bank ATM. The rest of the funds were exhausted through transactions conducted at Wal-Mart. All the transactions occurred at locations in and around Columbus, Ohio.

47. Person 29 was interviewed and stated that somebody siphoned money from his/her Citizen's Bank account through his/her USAA account. As soon as Person 29 discovered the theft, his/her spouse called USAA. USAA replaced the money immediately. Person 29 stated that he/she did not know Person 28.

48. PayPal records show that on June 9, 2017 at approximately 1:41 PM Central Daylight Time, $1,000 was transferred to PayPal xx7126 from a USAA Bank account belonging to Person 30. By 7:19 PM Central Daylight Time, all the funds had been exhausted through purchases made at various Wal-Mart stores in and around Columbus, Ohio.

49. USAA records show that the funds were transferred out of Person 30's bank account to somebody with the first initial matching that of Person 28's first name and the same last name as Person 28. The account was subsequently credited for the fraudulent transfer.

**Various Fraud Schemes - Money Laundering**

50. Through interviews and analysis of cell phones, financial records and other documentation, the affiant believes the investigation to date tends to show that Oduro and others have been engaged in a conspiracy to launder funds derived from various types of fraud schemes since at least June 2015.

51. According to bank records, Oduro opened JP Morgan Chase Bank account # xx8363 (JPMC xx8363) in June 2015. He was the only signer on the account.

52. According to records from the Ohio Secretary of State, Oduro established PW Logistics by filing an Articles of Organization with the Ohio Secretary of State located in Columbus, Ohio on February 12, 2016.

53. According to bank records, Oduro opened Branch Banking & Trust Company account xx4086 (BBT xx4086) in the name of PW Logistics, LLC in March of 2016. He was the only signer on the account.

54. According to bank records, Oduro opened Huntington Bank personal bank account xx0449 (HNB xx0449) on January 10, 2018. He was the only signer on the account.

55. According to bank records, Oduro opened Huntington Bank business bank account xx8943 (HNB xx8943) in the name of PW Logistics on August 29, 2018 at a bank branch located in Columbus, Ohio. He was the only signer on the account.

56. According to bank records, Oduro opened TD Bank personal bank account xx5247 (TD xx5247) on July 23, 2019. He was the only signer on the account.

57. According to bank records, Oduro opened TD Bank personal bank account xx3936 (TD xx3936) on August 14, 2019. He was the only signer on the account.

58. Law enforcement has interviewed or reviewed statements by several individuals who deposited, wired, or otherwise sent funds to bank accounts in the control of Oduro. Consideration of the witness statements and analysis of bank accounts in Oduro's control shows that between July 28, 2015 and March 10, 2020, Oduro received at least $630,000 in funds from victims of various fraud schemes. Oduro then conducted or caused to be conducted financial transactions to launder the fraud proceeds.

59. Review of the records of the bank accounts in Oduro's control did not result in finding revenue or expenses that would be typical of a business, such as customer payments, product purchases and regular payroll to other individuals.

*Person 12*

60. According to an interview with Person 12, whose identity is known to the affiant, Person 12 met somebody he/she believed to be named David Lucio through a contact he/she had made at a business meeting. Person 12 sent money at Lucio's request to a person he/she believed to be named Dr. Malik in London so that Lucio could have an operation. Person 12 also believed that he/she had mailed some checks to an address in Columbus, Ohio because he/she was investing in gold. The funds were not used for the stated purposes. Bank records show that, on July 28, 2015, Person 12 wired $57,623 to JPMC xx8363, controlled by Oduro. Bank records also show that, on April 5, 2016, Person 12 wired $3,125.19 to BBT xx4086, controlled by Oduro.

61. JP Morgan Chase Bank records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. July 29, 2015 – $1,000 Chase Quickpay transfer to Conspirator 4;

    b. July 29, 2015 – a second $1,000 Chase Quickpay transfer to Conspirator 4;

    c. July 29, 2015 - $1,900 cash withdrawal via ATM;

    d. July 29, 2015 - $40,000 transfer to a PNC Bank account held by Conspirator 4;

    e. July 30, 2015 - $7,000 transfer to a PNC Bank account held by Conspirator 4.

62. Branch Banking & Trust records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. April 7, 2016 - $800 cash withdrawal via ATM and an additional $3 fee;

b. April 7, 2016 - $1,000 wire to a PNC Bank account controlled by a third party.

*Person 13*

63. According to an interview with Person 13, whose identity is known to the affiant, Person 13 met somebody she believed to be named Scott Pace on a dating website in February of 2015. Pace was supposedly an American soldier who was in Afghanistan. After some time, Pace began asking Person 13 for various items then for money. Pace requested the money to pay hospital bills, for travel, and because he had found either diamonds or gold. Person 13 sent money to various accounts at Pace's direction. The funds were not used for the stated purpose. Bank records show that, on August 31, 2015, an official check issued by Person 13 in the amount of $20,000 was deposited into JPMC xx8363, controlled by Oduro.

64. Bank records show that, after receiving the funds and on or about the date set forth below, Oduro conducted the following financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. September 1, 2015 - $3,000 cash withdrawal via ATM.

*Person 7*

65. According to an interview with Person 7, whose identity is known to the affiant, Person 7 met somebody she believed to be named Peter Graham on a dating website a few years prior to 2017. Graham told Person 7 he was building a road in Dubai and needed Person 7 to send him money to do so. Graham instructed Person 7 to send money to various "intermediaries" including PW Logistics to pay for supplies to build the roads. Person 7 sent funds as directed by Graham. Bank records show that on June 28, 2016, Person 7 wired $95,000 to BBT xx4086.

66. Bank records show that, after receiving the funds, Oduro transferred $24,000 to another account he controlled at Branch Banking & Trust. Branch Banking & Trust reversed the account transfer and returned $91,370.13 to Person 7.

*Person 38*

67. According to an interview with Person 38, whose identity is known to the affiant, Person 38 received an email from a company she believed to be named Horizon Cargo Shipping in late 2017. The email informed Person 38 that her late husband, who had died in 2009, had allegedly stored valuable artwork and other items in Atlanta, Georgia. The story seemed plausible to Person 38 because her husband had travelled extensively. Person 38

sent money to Oduro and others in relation to attempts to receive these assets. The funds were not used for the stated purpose.

68. Bank records show that, on September 17, 2018, Person 38 wired $100,000 to HNB xx8943, controlled by Oduro.

69. Bank records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. September 18, 2018 - $5,000 transfer to HNB xx0449;

    b. September 19, 2018 - $20,000 check issued to company controlled by a third party;

    c. September 24, 2018 - $6,000 transfer to HNB xx0449;

    d. October 3, 2018 - $6,000 cash withdrawal at a bank branch located in Westerville, Ohio;

    e. October 4, 2018 - $8,000 cash withdrawal at a bank branch located in Westerville, Ohio;

    f. October 9, 2018 - $4,000 cash withdrawal at a bank branch located in Westerville, Ohio;

    g. October 9, 2018 - $20,000 check issued to a company controlled by a third party;

    h. October 12, 2018 - $2,000 cash withdrawal at a bank branch located in Westerville, Ohio;

    i. October 18, 2018 - $3,000 transfer to HNB xx0449.

70. Bank records show that, on November 28, 2018, Person 38 wired $25,000 to HNB xx8943, controlled by Oduro.

71. Bank records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. November 29, 2018 - $15,000 check issued to a company controlled by a third party;

    b. November 30, 2018 - $2,000 transfer to HNB xx0449.

72. Bank records show that, after receiving the funds described above into HNB xx0449 and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. December 3, 2018 - $340 cash withdrawal from an ATM located in Columbus, Ohio;

    b. December 3, 2018 - $200 cash withdrawal from an ATM located in Columbus, Ohio.

73. Bank records show that, on January 16, 2019, Person 38 wired $10,000 to HNB xx8943, controlled by Oduro.

74. Bank records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. January 22, 2019 - $500 transfer to HNB xx0449;

    b. January 22, 2019 - $400 transfer to HNB xx0449;

    c. January 28, 2019 - $600 transfer to HNB xx0449;

    d. February 1, 2019 - $2,000 cash withdrawal at a bank branch located in Columbus, Ohio;

    e. February 4, 2019 - $460 cash withdrawal at an ATM located in Columbus, Ohio;

    f. February 5, 2019 - $500 cash withdrawal at an ATM located in Columbus, Ohio.

75. Bank records show that, on April 26, 2019, Person 38 wired $63,800 to HNB xx8943, controlled by Oduro.

76. Bank records show that, after receiving the funds and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. April 29, 2019 - $3,900 transfer to HNB xx0449;

    b. April 29, 2019 - $900 transfer to HNB xx0449;

    c. April 29, 2019 - $11,500 issuance of a check payable to a shipping company;

d. May 2, 2019 - $2,000 transfer to HNB xx0449;

e. May 7, 2019 - $16,846 purchase of an official check payable to an online automobile auction company;

f. May 9, 2019 - $3,000 transfer to HNB xx0449;

g. May 28, 2019 - $1,000 transfer to HNB xx0449;

h. May 28, 2019 – a second $1,000 transfer to HNB xx0449;

i. June 3, 2019 - $2,000 transfer to HNB xx0449;

j. June 4, 2019 - $2,000 cash withdrawal;

k. June 5, 2019 - $1,000 transfer to HNB xx0449;

l. June 11, 2019 - $1,200 transfer to HNB xx0449;

m. July 3, 2019 - $1,500 transfer to HNB xx0449;

n. July 8, 2019 - $1,100 transfer to HNB xx0449.

77. Bank records show that, after receiving the funds detailed above into HNB xx0449 and on or about the dates set forth below, Oduro conducted the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. April 29, 2019 - $700 transfer via Wave, a digital remittance company;

b. April 20, 2019 - $1,330 transfer via Zelle, a digital remittance company;

c. May 1, 2019 - $200 cash withdrawal at an ATM located in Columbus, Ohio;

d. May 10, 2019 - $1,000 transfer via Wave;

e. May 10, 2019 - $500 transfer via Wave;

f. May 28, 2019 - $1,000 transfer via Zelle;

g. May 28, 2019 – a second $1,000 transfer via Zelle;

h. June 3, 2019 - $500 transfer via Wave;

i. June 3, 2019 - a second $500 transfer via Wave;

j. June 12, 2019 - $700 transfer via Wave;

k. June 12, 2019 - $400 transfer via Wave;

l. July 3, 2019 - $525 transfer via Zelle.

78. Bank records show that between September 25, 2019 and March 10, 2020, Person 38 wired $50,000 to TD xx5247 and a total of $100,000 to TD xx3936, both controlled by Oduro. Bank records also show that, after receiving the funds, Oduro conducted additional financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Such transactions continued through at least October 13, 2020.

## Use of Electronic Devices

**Pen Register and Trap and Trace**

79. Between September 20, 2019 and November 14, 2019, IRS-CI placed pen registers and trap and trace devices on several WhatsApp phone numbers, including 614-209-4594. Oduro provided this phone number to TD Bank when he opened TD xx3936 in August 2019. The results showed that during the time period covered, Oduro used WhatsApp on a regular basis to communicate with numbers based in the United States as well as numbers based in Ghana. The communications sent and received included text messages, audio files, video files and image files.

80. I know from investigative experience that WhatsApp is a smart phone application which can also be accessed via a computer. WhatsApp is a free instant messaging and voice over internet protocol service. The user of the application downloads the application to their phone and/or computer, and the application requires the user to assign a phone number to the application. After a phone number is assigned to the application, the application sends a verification text to the phone number assigned. In this way, the application is linked to the phone number of the phone onto which the application was downloaded.

81. I also know that smart phone applications such as WhatsApp, Hushed and Telegram are often installed on the phones of the perpetrators of fraud schemes such as this. These applications are used by persons engaged in fraud to communicate with individuals while potentially disguising their true identities. These communications can include communications with co-conspirators as well as victims.

**Further Information Regarding Prior Search Warrant on Oduro's Phone**

82. The prior search warrant executed on Oduro's phone taken during the execution of the search warrant by the Grove City Police Department on May 3, 2017 revealed that Oduro

used his phone to communicate with others about fraud schemes in which he was involved and perpetrated or attempted to perpetrate fraud schemes using his phone. Some of those instances have been detailed previously in this affidavit. Additional instances include:

a. On February 7, 2016, Oduro engaged in a conversation with a third party via WhatsApp. Oduro stated, "Half of the time I'm in a tie, even when I go to withdraw my fraud money…"

b. On February 8, 2016, Oduro engaged in a conversation with a third party via WhatsApp. Oduro stated, "This is the only business in America I can do and make 20k in a month and not get arrested…I'm locating money, I'm not fraud anyone…It's called money laundering."

c. On March 8, 2016, Oduro engaged in a conversation via WhatsApp with a third party. During the conversation, Oduro asked the third party if he needed a bank statement. The third party replied that Oduro did not need a bank statement. Oduro replied, "Okay because my bank statement de3 (sic) fraud written all over it…Lol but I'm trying to keep one clean account for this year."

d. From approximately September through November of 2016, Oduro engaged in conversations with a would-be victim via a text messaging application on his phone. Oduro assumed the identity of Caroline Emily Randolph. The conversation was entirely predicated upon a supposed romantic relationship between the would-be victim and "Randolph." During the conversation, "Randolph" requested money and electronics from the would-be victim numerous times.

e. The call log indicated that Oduro was in communication numerous times between April 26, 2016 and March 23, 2017 with a number which open-source information indicated belonged to Person 12.

f. Between October 18, 2016 and March 16, 2017, Oduro engaged in a conversation via a messaging app with another party. During the conversation on November 10, 2016, Oduro sent messages simply saying Person 12's true name and "James Randolph."

g. On March 1, 2017, Oduro sent three messages via a messaging app to a number which open-source information indicates belonged to Person 12. The first message informed Person 12 that his email address was jrand76110@gmail.com. The second message said, "Love you James." The third message implored Person 12 to find a way to communicate with him without his/her children knowing.

**Apple Records and iCloud Search Warrant**

83. The affiant reviewed records provided by Apple. The records showed that Apple IDs poduro55@icloud.com and poduro56@icloud.com are associated with Oduro.

84. On October 29, 2020, the affiant applied for and was granted search warrants for information associated with poduro55@icloud.com and poduro56@icloud.com and held by Apple on the "iCloud." The warrant was executed on November 2, 2020.

85. As a result of the search warrant, Apple provided records for poduro55@icloud.com. The records showed that Oduro maintained the following items, among thousands of other files, in his account:

    a. Numerous pictures of Oduro, alone and with others, dated at least as late as September 2019;

    b. Numerous images, which appear to be modified or "photo-shopped," showing a middle-aged man, some of which depict him in a hospital bed and gown. I know from investigative experience that it is common for scammers to use photos such as these when they create and assume false identities in order to perpetrate scams, especially romance scams.

    c. Numerous images of banking activity in various bank accounts at least as late as October 2019;

    d. Screenshots of text message conversations which I know from investigative experience to be typical of conversations that occur between scammers and money launderers and scammers and victims of romance fraud. Such screenshots included, but we not limited to:

        i. A conversation involving "Michael Morgan," who appears to be a fictitious person, and an unidentified individual during which Morgan tells the other individual, "How do I safely give your father's attorney $15,000…What would happen if I hand carried a cashier's check to Ghana and delivered it to your attorney." The unidentified individual responds, "…Michael am your lover, I trusted you from the beginning that's why I told you about my inheritance." Metadata indicates that the file was created on February 20, 2019.

        ii. A conversation involving "Fiona Asikas," who appears to be a fictitious person, and an unidentified individual during which the unidentified individual asks Asikas, "So should I send here (sic) address so that you can send the money to her my love…I think it will be better if you send it through western union to her my love." Asikas replies, "Okay my sweetheart." Metadata indicates that the file was created on February 20, 2019.

iii. A conversation involving two unidentified individuals during which unidentified individual # 1 says, "The man wan to send $15K…Ebi scam to make them relax…I mean Ebi scam we dey do…So we for do anything take the money." Unidentified individual # 2 responds, "Are you sure the client is going to send?" Metadata indicates that the file was created on June 14, 2019.

86. As a result of the search warrant, Apple provided records for poduro56@icloud.com. The records showed that Oduro maintained the following items, among thousands of other files, in his account:

a. Numerous pictures of Oduro, alone and with others, dated at least as late as February 8, 2020;

b. Numerous images showing middle-aged men, some of which appear to be photo-shopped and appear to be the same man referenced in paragraph # 85. I know from investigative experience that it is common for scammers to use photos such as these when they create and assume false identities in order to perpetrate scams, especially romance scams.

c. Numerous images of banking activity related to various bank accounts at least as late as September 10, 2020, including images of cashier's checks purchased by Person # 38.

d. Screenshots of text message conversations which I know from investigative experience to be typical of conversations that occur between scammers and money launderers and scammers and victims of romance fraud. Such screenshots included, but we not limited to:

i. A conversation involving Person 41, who appears to be a potential victim, and an unidentified individual during which the unidentified individual says, "I love you too honey…I am not going to get back all the money I have spent on this contract if I don't finish it in time…" Person 41 responds, "Don't do this to me. I really care about you. I don't have the (money) to give you…I don't send or give money go anyone." Metadata indicates that the file was created on January 7, 2020.

ii. A conversation involving two unidentified individuals during which unidentified individual # 1 sends unidentified individual # 2 banking information for a third-party then says, "Bro…This is the beginning." Unidentified individual # 2 responds, "Boys make wild ok…we dey for you…you for try to increase the percentage because me and chairman can't share 200$ lol." Metadata indicates that the file was created on July 14, 2020.

iii. A conversation involving the same two individuals during which unidentified individual # 2 says, "Client or wire?" Unidentified individual # 1 responds, "Click direct deposit…56k…my man, old client." Metadata indicates that the file was created on February 26, 2020.

**Technical Background**

87. Based upon my training and experience, I use the following technical terms to convey the following meanings:

a. Cell Phone/Mobile Device: A cell phone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

88. Based upon my training, experience and research, I know that the device for which the warrant is requested has capabilities to allow it to serve as a cell phone, digital camera, portable media player, GPS navigation device and PDA.

89. I have consulted with IRS-CI Special Agent-Computer Investigative Specialist Ebenger-Balla regarding the aspects of properly retrieving and analyzing electronically stored digital data. Special Agent Ebenger-Balla has been employed with IRS-CI since 2009. In addition to attending training in financial investigation techniques and accounting, she also completed the IRS-CI Basic Computer Evidence Recovery Training class at the Federal Law Enforcement Training Center in Glynco, Georgia, (2016) and the Advanced Computer Evidence Recovery Training class at the CyberCrimes Center in Fairfax, Virginia (2017), and Macintosh Forensics Training in Glynco, Georgia (2017). Special Agent Ebenger-Balla also completed the Mobile Device Forensics Training in Glynco, Georgia (2017) where she learned about the operation of mobile devices and the correct procedures for seizing and analyzing those devices.

90. Based upon the affiant's knowledge, training, experience and consultation with Special Agent Ebenger-Balla, the affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

91. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

    a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

    b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

    c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

    d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

    e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium

92. The affiant knows that searching and seizing information from computers and cell phones often requires agents to seize most or all electronic storage devices to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

    a. Technical requirements: Searching computer systems, such as cell phones, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to

complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

b. The volume and nature of electronic evidence: The volume of evidence. Computer storage devices such as cell phones can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

93. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

## Conclusion

94. Based on the information presented in this affidavit, I contend there is probable cause to believe that Oduro committed Bank Fraud, in violation of 18 USC 1344; Aggravated Identity Theft, in violation of 18 USC 1028A; and Money Laundering in violation of 18 USC 1956(a)(1)(B)(i) and 18 USC 1957. I further believe that Oduro and others used various electronic devices, namely their cell phones, to communicate regarding and to facilitate the fraud schemes and laundering of funds derived from fraud schemes, and evidence of these violations, as well as violations of 18 U.S.C. § 1343, is now located in the item described in Attachment A. Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Shawn A. Mincks
Special Agent, IRS-CI

ATTESTED TO BY FACETIME NMK

Subscribed and ~~sworn to before me~~

This 30th day of MARCH, 2022.

Norah McCann King
United States Magistrate Judge

**NORAH McCANN KING**
***United States Magistrate Judge***

# ATTACHMENT A

The property to be searched is a silver and white iPhone cell phone seized during the arrest of Prince Oduro on February 15, 2022.

Hereinafter, this cellular phone will be referred to as "the Device." The Device is currently located at 401 North Front Street, Suite 375, Columbus, Ohio.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

# ATTACHMENT B

1. All records on the Device described in Attachment A that are evidence of violations of Bank Fraud, in violation of 18 U.S.C. § 1344; Wire Fraud, in violation of 18 U.S.C. § 1343; Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A; Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); and Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957; for the period March 1, 2015, to the present, including:

   a. Records related to the wire-fraud schemes; bank-fraud schemes; identity-theft schemes; and money-laundering scheme described in the Affidavit;

   b. Records identifying the establishment, ownership, operation and/or control of any limited liability corporation or other business entity including articles of organization; correspondence with and/or submissions to/from any Secretary of State office; applications, disposition records and/or correspondence related to the issuance or use of Employer Identification Numbers (EIN); minutes and other official business records; and documents identifying any registered agent(s), incorporator(s), and/or other identified members;

   c. All records related to or referencing electronic transfers of funds or cash deposits including requests for an electronic transfer or cash deposit, wiring or deposit instructions, receipts, and correspondence;

   d. All records related or referring to persons or entities in other countries and the locations of such persons or entities;

   e. Asset ownership and/or acquisition records including contracts, invoices, receipts, registrations, titles insurance records and/or photographs of assets including motor vehicles, real property, boats, jewelry, precious metals and gems, and currency (foreign, domestic, or virtual currency);

   f. Travel records including travel directions, hotel reservations, rental car reservations, airplane reservations, invoices, airline tickets, and itineraries;

   g. Records related to banking activity including communications and data related to the opening, closing, use, custody and/or control of bank accounts, alternative currency accounts (i.e. those related to Bitcoins), credit cards, and/or debit cards including applications for accounts; approval or declination notices; credit and/or debit card issuance notices; credit and/or debit card activations; bank statements; welcome or account opening/closing notifications; deposit, payment, withdrawal, or transfer orders, receipts and/or notifications; balance inquiries and/or notices; and security notifications;

h. All financial statements, accounting records and supporting source documents relating to receipts, expenditures, general ledgers, accounts and notes receivable, accounts and notes payable, balance sheets, income statements, statements of profit and loss, and any other accounting records and other records and/or ledgers relating to PW Logistics or any variation of these entity names or any other entities identified through items seized pursuant to section a. above;

i. Records pertaining to any financial institution account including but not limited to account numbers, passwords, personal identification numbers (PINS), deposit/withdrawal records, notes, logs, and photographs;

j. Electronic records of internet sites visited and data accessed and/or communications made in the course of visiting such internet sites;

k. Communications records and histories made through and/or from applications (known as "Apps"); emails; texts; calls or other media contained on the electronic devices to be searched and all attachments included in such communications; and

l. Contact lists and any documents reflecting names, addresses, email addresses, telephone numbers, fax numbers and/or other contact information.

m. Evidence indicating the cell phone owner's or user's state of mind as it relates to the crimes under investigation.

2. Evidence of user attribution showing who used or owned the cell phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.